1 **CLAIMS**

ļ. 4

- Having thus described my invention, what I claim as new and desire to secure by Letters 2
- Patent is as follows: 3
- 1. A method for encrypting a plain-text message, the method comprising: 4
- 5 generating a first random number;
- transforming said first random number into a first pseudo random number; 6
- further expanding a randomness of said first random number and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers;
 - dividing said plain-text message into a plurality of plain-text blocks;
 - encrypting said plain-text blocks to form a plurality of cipher-text blocks;
 - combining said plurality of plain-text blocks into at least one check sum; and
 - employing said set of pair-wise differentially-uniform pseudo random numbers, together 12
 - with said first random number and/or said first pseudo random number, to embed a 13
 - message integrity check in said cipher-text blocks. 14
 - 2. A method as recited in claim 1, wherein the step of encrypting said plain-text blocks 15
 - includes employing the said first random number, and/or said first pseudo random 16
 - number, and/or said set of pair-wise differentially-uniform pseudo random numbers. 17

- 3. A method as recited in claim 1, wherein the step of employing includes pairing said
- 2 first random number, and/or said first pseudo random number, and/or said set of pair-wise
- differentially-uniform pseudo random numbers, with said plurality of cipher-text blocks;
- 4 and
- 5 combining each pair to form a plurality of output blocks.
- 4. A method as recited in claim 3, wherein the step of combining each pair includes
- 7 performing an exclusive-or operation upon components of said each pair.
- 8 5. A method as recited in claim 1, wherein the step of encrypting includes encrypting
- said first random number.

 6. A method as recited in check sum.

 7. A method as recited in check sum from an exclusion of the check sum from the check
 - 6. A method as recited in claim 1, wherein the step of encrypting includes encrypting said check sum.
 - 7. A method as recited in claim 1, wherein the step of combining includes obtaining said check sum from an exclusive-or of said plurality of plain-text blocks.
 - 8. A method as recited in Claim 1, wherein the step of transforming said random number includes a non-cryptographic or linear operation.
 - 9. A method as recited in Claim 1, wherein the step of transforming said random number
 - includes a cryptographic operation.
 - 18 10. A method as recited in Claim 1, wherein the said set of pair-wise
 - differentially-uniform numbers are set of pair-wise differentially-uniform numbers in
 - 20 GFp.
 - 21 11. A method as recited in claim 2, wherein the step of employing includes:

- pairing said first random number, and/or said first pseudo random number, and/or said set 1
- of pair-wise differentially-uniform pseudo random numbers, with said plurality of 2
- plain-text blocks; and 3

- combining each pair to form a plurality of input blocks used in said step of encrypting. 4
- 12. A method as recited in claim 11, wherein the step of combining each pair includes 5
- performing an exclusive-or operation upon components of said each pair. 6
- 7 13. A method for decrypting a cipher-text message, the method comprising:
- dividing said cipher-text message into a plurality of cipher-text blocks;
 - decrypting said cipher-text blocks in forming a plurality of plain-text blocks;
 - transforming at least one of said plain-text blocks into a first pseudo random number;
 - further expanding at least one of said plain-text blocks and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers;
 - combining said first pseudo random number, and/or said set of pair-wise 13
 - differentially-uniform pseudo random numbers, and/or said at least one plain-text block 14
 - to form at least two check sums and to form a plurality of output blocks; and 15
 - comparing said at least two check sums in declaring success of a message integrity check. 16
 - 17 14. A method as recited in claim 13, wherein the step of decrypting said cipher-text
 - 18 blocks includes employing said first pseudo random number, and/or said set of pair-wise
 - 19 differentially-uniform pseudo random numbers.

- 15. A method as recited in claim 13, wherein the step of combining includes: 1
- pairing said first pseudo random number, and/or said set of pair-wise 2
- differentially-uniform pseudo random numbers, with said plurality of plain-text blocks; 3
- and 4
- using each pair to form a plurality of output blocks and employing the output blocks to 5
- form said at least two check sums. 6
- 16. A method as recited in claim 15, wherein the step of using each pair includes 7 performing an exclusive-or operation upon components of said each pair. 8
- 17. A method as recited in claim 15, wherein the step of forming includes:
 - dividing the said output blocks into at least two subsets, and
 - obtaining said at least two checksums from an exclusive-or of said subsets of output blocks.
- 12 13 18. A method as recited in Claim 13, wherein the step of transforming said plain-text
- 14 blocks includes a non-cryptographic or linear operation.
- 19. A method as recited in Claim 13, wherein the step of transforming said plain-text 15
- blocks includes a cryptographic operation. 16
- 20. A method as recited in Claim 13, wherein the said set of pair-wise 17
- differentially-uniform numbers are set of pair-wise differentially-uniform numbers in 18
- 19 GFp.

- 1 21. A method as recited in claim 14, wherein the step of employing includes:
- 2 pairing said first random number, and/or said first pseudo random number, and/or said set
- of pair-wise differentially-uniform pseudo random numbers, with said plurality of
- 4 cipher-text blocks; and
- 5 combining each pair to form a plurality of input blocks used in said step of decrypting.
- 6 22. A method as recited in claim 3, wherein p is a prime number, and the step of
- 7 combining each pair includes performing a modulo p addition upon components of said
- 8 each pair.

- 23. A method as recited in claim 11, wherein p is a prime number, and the step of combining each pair includes performing a modulo p addition upon components of said each pair.
- 24. A method as recited in claim 15, wherein p is a prime number, and the step of using each pair includes performing a modulo p addition upon components of said each pair.
- 25. A method as recited in claim 21, wherein p is a prime number, and the step of combining each pair includes performing a modulo p addition upon components of said each pair.
- 17 26. An article of manufacture comprising a computer usable medium having computer
- readable program code means embodied therein for causing encryption of a plain-text
- message, the computer readable program code means in said article of manufacture
- 20 comprising computer readable program code means for causing a computer to effect the
- 21 steps of claim 1.

- 1 27. An article of manufacture comprising a computer usable medium having computer
- 2 readable program code means embodied therein for causing decryption of a cipher-text
- 3 message, the computer readable program code means in said article of manufacture
- 4 comprising computer readable program code means for causing a computer to effect the
- 5 steps of claim 13.
- 6 28. A computer program product comprising a computer usable medium having
- 7 computer readable program code means embodied therein for causing encryption of a
- 8 plain-text message, the computer readable program code means in said computer program
- 9 product comprising computer readable program code means for causing a computer to
- effect the steps of claim 1.
- 29. A computer program product comprising a computer usable medium having
 - computer readable program code means embodied therein for causing decryption of a
 - plain-text message, the computer readable program code means in said computer program
- product comprising computer readable program code means for causing a computer to
- effect the steps of claim 13.

ļ. <u>4</u>

- 30. A program storage device readable by machine, tangibly embodying a program of
- instructions executable by the machine to perform method steps for encrypting a
- plain-text message, said method steps comprising the steps of claim 1.
 - 19 31. A program storage device readable by machine, tangibly embodying a program of
 - 20 instructions executable by the machine to perform method steps for decrypting a
 - cipher-text message, said method steps comprising the steps of claim 13.
 - 32. A method for encryption/decryption of a plain-text message, the method comprising
 - 23 the steps of:
 - 24 generating a first random number;

- transforming said first random number into a first pseudo random number;
- 2 further expanding a randomness of said first random number and/or said first pseudo
- 3 random number into a set of pair-wise differentially-uniform pseudo random numbers;
- 4 dividing the plain-text message into a plurality of plain-text blocks;

- 5 encrypting said plain-text blocks in forming a plurality of cipher-text blocks;
- 6 combining said plurality of plain-text blocks into at least one check sum; and
 - employing said first random number, said first pseudo random number and said set of pair-wise differentially-uniform pseudo random numbers to embed a message integrity check in said cipher-text blocks to form a cipher-text message; and
 - dividing said cipher-text message into a plurality of cipher-text blocks to form an encryption of said plain-text message;
 - decrypting said cipher-text blocks in forming a plurality of plain-text blocks;
- transforming at least one of said plain-text blocks into a first pseudo random number;
- further expanding at least one of said plain-text blocks and/or said first pseudo random
- number into a set of pair-wise differentially-uniform pseudo random numbers;
- combining said first pseudo random number, and/or said set of pair-wise
- differentially-uniform pseudo random numbers, and/or said at least one plain-text block
- to form at least two check sums and to re-form the said plain-text message; and

- 1 comparing said at least two check sums in declaring success of a message integrity check
- 2 in decryption of said cipher-text to reform said plain-text message.
- 3 33. An apparatus to encrypt a plain-text message, the apparatus comprising:
- 4 a Randomness Generator to generate a first random number;
- 5 a Randomness Transformer to transform said first random number into a first pseudo
- 6 random number;
- 7 a Pairwise Additively Uniform Sequence Generator to further expand a randomness of
 - said first random number and/or said first pseudo random number into a set of pair-wise
 - differentially-uniform pseudo random numbers;
 - an Encryptor to divide said plain-text message into a plurality of plain-text blocks, and to
 - encrypt said plain-text blocks to form a plurality of cipher-text blocks;
 - a Checksum Generator to combine said plurality of plain-text blocks into at least one
- check sum; and

- 12 13 14 14 an Integrity Extractor and Checker to employ said set of pair-wise differentially-uniform
 - pseudo random numbers, together with said first random number and/or said first pseudo 15
 - 16 random number, to embed a message integrity check in said cipher-text blocks.
 - 17 34. An apparatus to decrypt a cipher-text message, the apparatus comprising:
 - a Decryptor to divide said cipher-text message into a plurality of cipher-text blocks, and 18
 - 19 to decrypt said cipher-text blocks in forming a plurality of plain-text blocks;

- a Randomness Transformer to transform at least one of said plain-text blocks into a first
- 2 pseudo random number;
- a Pairwise Additively Uniform Sequence Generator to further expand at least one of said
- 4 plain-text blocks and/or said first pseudo random number into a set of pair-wise
- 5 differentially-uniform pseudo random numbers;
- 6 a Checksum Generator to combine said first pseudo random number, and/or said set of
- 7 pair-wise differentially-uniform pseudo random numbers, and/or said at least one
- 8 plain-text block to form at least two check sums and to form a plurality of output blocks;
- 9 and

17

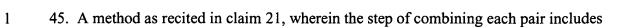
18

19

20

- an Integrity Extractor and Checker to compare said at least two check sums in declaring success of a message integrity check.
- 35. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 2.
- 36. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing decryption of a cipher-text message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 14.
- 37. A computer program product comprising a computer usable medium having
 computer readable program code means embodied therein for causing encryption of a
 plain-text message, the computer readable program code means in said computer program

- product comprising computer readable program code means for causing a computer to 1
- 2 effect the steps of claim 2.
- 3 38. A computer program product comprising a computer usable medium having
- 4 computer readable program code means embodied therein for causing decryption of a
- 5 plain-text message, the computer readable program code means in said computer program
- 6 product comprising computer readable program code means for causing a computer to
- 7 effect the steps of claim 14.
- 8 39. A program storage device readable by machine, tangibly embodying a program of
- 9 instructions executable by the machine to perform method steps for encrypting a
- plain-text message, said method steps comprising the steps of claim 2.
 - 40. A program storage device readable by machine, tangibly embodying a program of
 - instructions executable by the machine to perform method steps for decrypting a
 - cipher-text message, said method steps comprising the steps of claim 14.
 - 41. A method as recited in claim 3, wherein the step of combining each pair includes
 - performing an addition in a group upon components of said each pair.
- 42. A method as recited in claim 11, wherein the step of combining each pair includes
 - performing an addition in a group upon components of said each pair 17
 - 43. A method as recited in claim 15, wherein the step of using each pair includes 18
 - performing an addition in a group upon components of said each pair. 19
 - 44. A method as recited in claim 21, wherein the step of combining each pair includes 20
 - performing an exclusive-or operation upon components of said each pair. 21



2 performing an addition in a group upon components of said each pair.